DEPARTMENT OF REAL ESTATE
2201 Broadway
Sacramento, CA 95818
(916) 227-0782

December 31, 2009

DALE E. BONNER
Secretary
Business, Transportation and Housing Agency
980 Ninth Street, Suite 2450
Sacramento, CA 95814

Dear Secretary Bonner:

Pursuant to the Financial Integrity and State Manager's Accountability Act of 1983 and State Administrative Manual (SAM) Section 20060, the Department of Real Estate has conducted a study and evaluation of the accounting and administrative controls in effect on June 30, 2009.

The study and evaluation was conducted in accordance with the Standards for the Professional Practice of Internal Auditing by the Institute of Internal Auditors, Inc., and using the "Guidance for the Evaluation of Internal Control" published by the California Department of Finance.

The enclosed Internal Control Transmittal letter and report are being provided to you in accordance with SAM Section 20060. If you have any questions concerning the report, please contact Daniel J. Sandri, Supervising Auditor II at (510) 622-2531, or me at (916) 227-0782.

Sincerely,

JEFF DAVI
Real Estate Commissioner

cc. Office of Governor Arnold Schwarzenegger
Michael Tritz, Deputy Secretary for Audits and Performance Improvement, BTH Agency
Barbara Bigby, Chief Deputy Commissioner, Department of Real Estate
Fa-Chi Lin, Chief Auditor, Department of Real Estate
Daniel Sandri, Supervising Auditor, Department of Real Estate

Submitted electronically to:

FISMAhotline@dof.ca.gov
Katarina.Tarr@asm.ca.gov
MargaritaF@bsa.ca.gov
RFontaine@library.ca.gov

INTERNAL AUDIT REPORT

DEPARTMENT OF

DRE

REAL ESTATE

2009

AGENCY NAME: Business, Transportation, and Housing
DEPARTMENT NAME: Department of Real Estate
ORGANIZATION CODE: 2320

INTRODUCTION:
In accordance with the Financial Integrity and State Managers Accountability (FISMA) Act of 1983, the Department of Real Estate submits this report of the review of our systems of internal control for the biennial period ended December 31, 2009.

Should you have any questions, please contact Daniel J. Sandri, Supervising Auditor II, at (510) 622-2531 or via e-mail at Dan_Sandri@dre.ca.gov

BACKGROUND:
Mission and Goals:
The Mission of the Department of Real Estate (the Department) is: *To protect and serve the interests of the public in real estate transactions and provide related services to the real estate industry.* The governance of the Department is structured with core values that promote independence and balance between its two distinct mission responsibilities. These values preserve the integrity of operational obligations, ensure coordination and cooperation between the operating programs, engage Department stakeholders, and foster an environment that supports the professional development of its staff.

The strategic goals of the Department that support its mission are to:

1. Enhance consumer awareness and protection.
2. Assess and improve services.
3. Promote workforce excellence.

Department Structure:
The core functions of the Department are to administer license examinations, issue real estate licenses, provide consumer protection, regulate real estate licensees, and qualify subdivision offerings.

The Department is a special fund agency that derives virtually all its revenues from examination, license and subdivision fees. It has limited authority to fine and, as a result, regulatory related fines compose less than one percent of its budget. Fines collected by the Department are paid into the Recovery Account to help compensate victims of real estate fraud.

The Department maintains five offices: Sacramento, Oakland, Fresno, Los Angeles, and San Diego, and as of June 30, 2009, has 341 authorized positions. As of October 31, 2009, there were approximately 509,000 real estate licensees in California.

The Real Estate Commissioner is the chief executive officer of the Department. It is the Commissioner's responsibility to determine administrative policy and enforce the provisions of the Real Estate Law for the protection of the public. The Commissioner is appointed by the Governor and reports directly to the Secretary of the Business, Transportation and Housing Agency.

The Department is divided into various divisions that are managed by program managers (Assistant Commissioners), who report directly to the Commissioner and the Chief Deputy Commissioner. These divisions are as follows: Enforcement, Legal, Audits, Subdivisions, Legislation, Mortgage Lending and Public Information, and Administrative Services, which consists of Licensing, Information Systems, Fiscal and Human Resources.

Control Environment:

Integrity and Ethical Values: Management of the Department has established policies designed to encourage ethical behavior by all employees. Included, among others, in these policies are a Conflict of Interest Code and policies on Information Security, Equal Employment Opportunity, Sexual Harassment, Nepotism, Training, and Political Activities. All designated employees must complete an annual Statement of Economic Interests (FPPC Form 700). Employees are reminded at login on computer systems that information technology systems are to be used for business purposes only and are subject to monitoring. Employees are regularly required to take ethics training, sexual harassment training, and privacy training. Periodic reminders of policies, programs such as the Whistleblower Protection Act, as well as many other trainings are announced by the Commissioner. Other policy reminders, programs, and events of interest are regularly announced to employees through their respective program managers. Departures from approved policies and procedures, if of sufficient severity, may result in disciplinary action. Management has prepared a Disaster Recovery Plan, a Risk Management Plan, and a Continuity of Operations/ Continuity of Government Plan (COOP/COG).

Commitment to Competence: Duty statements/job descriptions are submitted to Human Resources by supervisors for all positions and employees. Once the duties are reviewed and approved, a copy is provided to each employee and Human Resources maintains a record of each duty statement. Classification studies and job analyses are performed and maintained to determine the knowledge and skills needed to perform particular jobs.

Management's Philosophy and Operating Style: Management, through establishment of controls, formal plans, and the use of internal audit, is vigilant in attempting to minimize risk. Personnel turnover in critical areas has been acceptable. Senior management reviews financial reports regularly. Management has a positive attitude towards internal audit and the function it plays.

The Department recognizes that effective Risk Management requires open, clear, and ongoing communication of threats within its programs. The Risk Management process draws on the existing program operations guidelines, the Department's Risk Management Program, emergency plans, and project documentation to the maximum extent possible.

Project related risks are assessed and tracked by the Project Manager and are project specific, configuration controlled, and include technical information by reference. The project risks are determined through the feasibility study report and are further refined during the phases of the project life cycle.

Organization Structure: The Department's program divisions are each very centralized, with managers/supervisors reporting to the program chief, who in turn reports to the Commissioner and the Chief Deputy Commissioner.

Managers and supervisors have clearly defined duties in their Duty Statements. The Department has a veteran and knowledgeable management staff with sufficient experience and training to fulfill their responsibilities. Reporting relationships are clearly defined.

Assignment of Authority and Responsibility: Duty statements/job descriptions are established for all management and supervisory personnel. Supervisors/Managers report to each program chief who in turn reports directly to the Commissioner and the Chief Deputy Commissioner.

Human Resource Policies and Practices: The Department has established policies and procedures regarding hiring, training and promoting employees. Management of the hiring section is actively involved in working with Human Resources during the hiring process. Training regarding data security and integrity is provided to all new employees and each employee acknowledges them in writing. Individual Development Plans are completed annually by supervisors on the employee's birthday month. Disciplinary actions for non-adherence to policies are judged on a case-by-case basis.

VACANT POSITIONS:
For the fiscal year ending June 30, 2009, the Department did not lose any vacant positions pursuant to Government Code Section 12439.

RISK ASSESSMENT:
Risk management is an organized, systematic decision-making process that efficiently identifies, analyzes, plans (for the handling of risks), tracks, controls, communicates and documents risk. Effective risk management increases the likelihood of achieving program/project success and maintaining continuous business operations.

Risk is characterized by the combination of the probability that a business operation, program or project will experience an undesired event (some examples include a cost overrun, schedule slippage, safety mishap, malicious activities, environmental impact, or failure) and the consequences, impact, or severity of the undesired event, were it to occur.

Risk management, therefore, is a process wherein Department program managers and/or project teams are responsible for identifying, analyzing, planning, tracking, controlling, and communicating effectively the potential risks and the steps identified to control or mitigate them by a project team or business owner. Risk Management is enhanced by the Department's organizational structure and establishment of positions whose duties are aimed at identifying, analyzing, planning (for the handling of risks), tracking, controlling, communicating and documenting risk. The Department has a Risk Management Committee composed of the Program Managers, the Information Security Officer, and the Chief Information Officer. The Department has established an Information Security Officer (ISO), who is responsible for coordinating the overall security efforts of the Department and represents top management on all issues bearing on security. On a functional basis, the ISO reports directly to the Commissioner and Chief Deputy Commissioner. The ISO is not a System Owner or Data Owner. The Department has also designated a Disaster Recovery Coordinator to represent the Department in the event of a disaster or other event resulting in the severe loss of information technology systems capability. The Department has also designated a Privacy Program Coordinator to certify that the Department is following state mandated privacy guidelines. This designee must have knowledge of how privacy data is used in the Department.

The purpose of the Department's Risk Management Program is to establish and maintain a standard of due care to prevent misuse or loss of the Department's information assets, protect confidential or sensitive information from unauthorized access, and define cost-effective approaches to managing these risks. The Risk Management Program applies to all offices and employees, as well as contractors in accordance with the extent specified in their respective contracts. As part of this program, the Department has prepared a Risk Management Report, as required by State Administrative Manual (SAM) Section 5305, that defines and/or establishes procedures that:

1) Assign responsibility for risk assessment;
2) Identify the Department's information assets that are at risk, with particular emphasis on the applications of information technology (IT) that are critical to program operations. As part of this process, IT applications are prioritized to ensure continued operation;
3) Identify threats to which the information assets could be exposed;
4) Assess the vulnerabilities, i.e., the points where information assets potentially lack sufficient protection from identified threats;
5) Determine the probable loss or consequences, based upon quantitative and qualitative evaluation, of realized threats and an estimation of the likelihood of such occurrence;
6) Identify and estimate the cost of protective measures which would eliminate or reduce the vulnerabilities to an acceptable level;
7) Identify the amount of remaining risks acceptable to the Department; *and,*
8) Select cost-effective security management measures to be implemented as required.

This Risk Management Program is designed to protect the information assets and information system components of the Department, as well as to prevent the unauthorized access to confidential and sensitive information in the Department's care.

The following seven principles of risk management, as published by Carnegie Mellon, summarize the framework the Department follows to achieve effective risk management.

Table 1: Principles of Risk Management

Global Perspective	• Viewing software development within the context of the larger systems-level definition, design, and development. • Recognizing both the potential value of opportunity and the potential impact of adverse effects.
Forward-looking View	• Thinking toward tomorrow, identifying uncertainties, anticipating potential outcomes. • Managing project resources and activities while anticipating uncertainties.
Open Communication	• Encouraging free-flowing information at and between all project levels. • Enabling formal, informal, and impromptu communication. • Using processes that value the individual voice (bringing unique knowledge and insight to identifying and managing risk).

Integrated Management	• Making risk management an integral and vital part of project management. • Adapting risk management methods and tools to a project's infrastructure and culture.
Continuous Process	• Sustaining constant vigilance. • Identifying and managing risks routinely through all phases of the project's lifecycle.
Shared Product Vision	• Mutual product vision based on common purpose, shared ownership, and collective communication. • Focusing on results.
Teamwork	• Working cooperatively to achieve common goal. • Pooling talents, skills, and knowledge.

By applying these principles and using lessons learned as a baseline, the Department has successfully incorporated the risk management methodology into its busines operations. Additionally, the Department monitors and refines its personnel policies as necessary to ensure the entire staff is cognizant of potential risk factors.

In addition to assessment of risk via preparation of the Risk Management Report, the Department, through its Internal Audit Unit, performs a risk assessment as part of the biennial FISMA audit. While also targeting information assets and the Department's privacy program, this risk assessment process includes the financial assets in its scope.

Accounting controls are reviewed by transaction cycles. In addition, the Department reviewed additional cycles that were specific to the Department's operations. The Internal Audit Unit analyzes each cycle and calculates a risk assessment factor based upon the sum of the extended Values divided by the Sum of the Significant Factors. Each risk factor is then ranked from 1 to 13 with 13 being the highest risked cycle. The greatest vulnerabilities, therefore, lie with the highest ranked cycles. The Department focused on each cycle, with more time allotted for the higher ranked cycles. In addition, the Department expanded its focus on reviewing the progress of its Electronic Examinations Project and its IT Infrastructure Replacement Project since a significant amount of resources has been allotted to these projects.

The Department's risk management methodology is designed to address both the continuity of operational program and project lifecycle risks. General guidelines derived from the methodology promote best practices including: identification of responsibilities, management, identification, and analytical review of risks; calculation of risk factors; and the establishment of practices to avoid, mitigate, or react in a contingency mode to the occurrence of critically defined risks.

An external audit was conducted by CalPERS in March 2009. The scope of the audit involved a review of the Department's payroll reporting and enrollment processes for compliance with CalPERS health and retirement mandates. A final report was received on August 24, 2009. The findings were corrected prior to the issuance of the final report.

A follow-up internal audit was performed by the Internal Audit Unit in July 2008 for items contained in the 2007 FISMA audit. The reportable weaknesses described in the 2007 FISMA audit report had been corrected.

EVALUATION OF RISKS AND CONTROLS:

Our review of the systems of internal control for the biennial period ended December 31, 2009 found the following reportable condition:

Issue #1

Condition - A review of the bank reconciliations as of March 31, 2009, April 30, 2009 and May 31, 2009 disclosed a lack of supporting documentation. SAM 7923 requires that Deposit in Transit figures be supported by a list of deposit number, date deposit posted and the amount. Agencies will attempt to resolve deposits in transit over 30 days. Errors on the bank statement will be corrected as provided in SAM 8060. The person reconciling the bank statement will trace every item between the bank and the agency's records and include an explanation on the reconciliation.

Risk - The risk of not having supporting documentation is high since errors by the bank or the Department may have occurred.

Corrective Action – Currently, reconciliation worksheets are prepared monthly showing listings of deposit numbers, dates and amounts. They also show listings of outstanding checks not cashed. The deposits in transit are designated by color shading on the worksheets. All items will be documented and reconciled properly.. A review of the bank reconciliation process will include current practices at other Departments where credit card/ZBA processing occur. The Department will make inquiries with Bank of America to more effectively utilize the daily report sent for the Zero Balance Account. The Department will become more familiar with the PayPal website to utilize some specialized criteria for pending transactions to document the reconciliation of the Zero Balance Credit Card. As a conclusion, the Department's bank reconciliation procedures will be revised.

CONCLUSION:

The objectives of accounting and administrative control are to provide management with reasonable, but not absolute, assurance that:

- Assets are safeguarded against loss from unauthorized use or disposition.
- Transactions are executed in accordance with management's authorization and recorded properly to permit the preparation of reliable financial statements.
- Financial operations are conducted in accordance with policies and procedures established in the State Administrative Manual.

The accounting and administrative control at the Department of Real Estate in effect for the fiscal year ending June 30, 2009, taken as a whole, was sufficient to meet the objectives stated above.